www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2 Issue 4 April, 2013 Page No. 962 -966

Secure Authentication Methods for Preventing Jamming Attacks In Wireless Networks

Y. Madhavi Latha[1] P. Rambabu[2]
M.Tech (CSE),
NIET, Ongole.
Associate Professor, CSE,
NIET, Ongole.

Abstract:

The open nature of the wireless average greeneries it susceptible to intended interfering attacks, typically referred to as blocking. This intended interfering with wireless transmissions can be used as a Launch pad for rising Denial-of-Service attacks on wireless networks. Typically, blocking has been addressed under an external threat model. However, adversaries with internal knowledge of protocol specifications and network secrets can launch low-effort blocking attacks that are difficult to detect and counter. In this work, we address the problem of selective blocking attacks in wireless networks. In these attacks, the adversary is active only for a short period of time, selectively directing messages of high importance. We illustrate the advantages of selective blocking in terms of network performance reduction and adversary effort by presenting two case studies; a selective attack on TCP and one on routing. We show that selective blocking attacks can be launched by performing real-time packet classification at the physical layer. To lessen these attacks, we develop three schemes that prevent real-time packet classification by combining cryptographic primitives with physical-layer attributes. We analyze the security of our methods and evaluate their computational and message overhead.

Index Terms— Jamming, Denial-of-Service, Wireless Networks, Packet Classification

I. INTRODUCTION

Wireless networks rely on the continuous availability of the wireless medium to connect contributing nodes. However, the open nature of this average greeneries it susceptible to multiple security threats. Someone with a transceiver can snoop on wireless transmissions, inject spurious messages, or gridlock genuine ones. While snooping and message injection can be banned using cryptographic methods, blocking attacks are much harder to counter. They have been shown to objectify severe Denial-of-Service (DoS) attacks against wireless networks. In the form of blocking, the opponent delays with the reception of messages by transmitting a continuous blocking signal, or several short blocking pulses. Typically, blocking attacks have been considered under an exterior threat model, in which the block is not part of the network. Under this model, blocking strategies include the continuous or random transmission of high-power interference signals. However, adopting an always on strategy has several disadvantages. First, the rival has to spend a significant amount of energy to jam frequency bands of interest. Second, the continuous presence of unusually high meddling levels makes this type of attacks easy to detect. Conventional anti jamming techniques rely extensively on spread-spectrum (SS) communications, SS techniques provide bit-level protection by dispersal bits

according to a secret pseudo noise (PN) code known only to the communicating parties. These methods can only protect wireless transmissions under the exterior threat model. Potential revelation of secrets due to node compromise defuses the gains of SS. Broadcast communications are particularly susceptible under an interior threat model because all intended receivers must be conscious of the secrets used to protect transmissions. Hence, the compromise of a single receiver is enough to reveal relevant cryptographic information .We address the problem of blocking under an interior threat model. We consider a sophisticated opponent who is aware of network secrets and the implementation details of network protocols at any layer in the network stack. The adversary exploits his interior knowledge for initiation discerning blocking attacks in which specific messages of high importance are targeted. For, a jammer can target route-request route-reply messages at the routing layer to stop route discovery, or target TCP acknowledgments in a TCP session to severely destroy the throughput of an end-to-end movement. To launch perceptive blocking attacks, the adversary must be capable of implementing classify then jam strategy before the completion of a wireless transmission. Such strategy can be actualized either by classifying transmitted packets using protocol semantics, or by decoding packets on the fly. In the latter method, the jammer may decode the first few bits of a packet for improving useful packet identifiers such as packet type, source and destination address. After classification, the adversary must induce a sufficient number of bit errors so that the packet cannot be recovered at the receiver . Discerning blocking requires an intimate knowledge of the physical layer, as well as of the specifics of upper layers.

II. TYPES OF JAMMER

Continuous blocking has been used as a denial-of-service (DoS) attack against voice communication since the 1940s. Recently, several alternative jamming strategies have been Categorized jammers into four models, (a) a constant jammer that continuously emits noise, (b) a deceptive jammer that continuously broadcasts fabricated messages or replays old ones, (c) a random jammer that alternates between periods of continuous jamming and inactivity, and (d) a reactive jammer who jams only when transmission activity is detected.

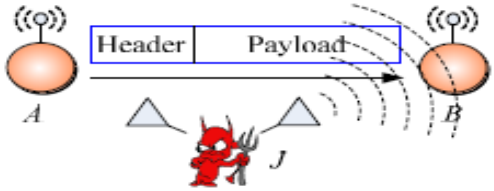

Fig1:Realization of a selective jamming attack

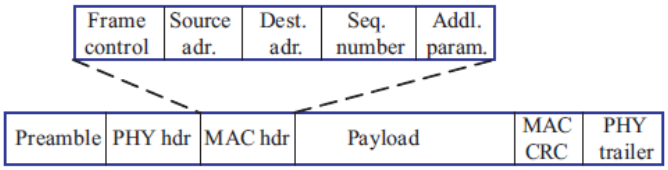

Fig 2: A generic frame format for a wireless network

A. Constant jammer

The constant jammer continually emits a radio signal. It has implemented a constant jammer using two types of devices. The first type of device to use is a waveform generator which continuously sends a radio signal. The second type of device it used is a normal wireless device. In this author, it will focus on the second type, which it built on the MICA2 Mote platform. This constant jammer continuously sends out random bits to the channel without following any MAC-layer etiquette. Specifically, the constant jammer does not wait for the channel to become idle before transmitting. If the underlying MAC protocol determines whether a channel is idle or not by comparing the signal strength measurement with a fixed threshold, which is usually lower than the signal strength generated by the constant jammer, a constant jammer can effectively prevent legitimate sources from getting hold of channel and sending packets.

B. Deceptive jammer

Instead of sending out random bits, the deceptive jammer constantly injects regular packets to the channel without any gap between subsequent packet transmissions. As a result, a normal communicator will be received into believing there is a legitimate packet and will be duped to remain in the receive state. For example, in Tiny OS, if a preamble is detected, a node remains in the receive mode, regardless of whether that node has a packet

to send or not. Hence, even if a node has packets to send, it cannot switch to the send state because a constant stream of incoming packets will be detected. Further, it also observe that it is adequate for the jammer to only send a continuous stream of preamble bits (0xAA in Tiny OS) rather than entire packets.

C. Random jammer

Instead of sending out a radio signal continuously, a random jammer alternates between sleeping and jamming. Specifically, after jamming for tj units of time, it turns on its radio, and enters a sleeping mode. It will resume jamming after sleeping for ts time. tj and ts can be either random or fixed values. During its jamming phase, it can either behave like a constant jammer or a deceptive jammer. Throughout this art hour, this random jammer will operate as a constant jammer during jamming. The distinction between this model and the previous two models lies in the fact that this model tries to take energy conservation into consideration, which is especially important for those jammers that do not have unlimited power supply. By adjusting the distribution governing the values of tj and ts, it can achieve various levels of tradeoff between energy efficiency and jamming effectiveness.

D.Reactive jammer

The three models discussed above are active jammers in the sense that they try to block the channel irrespective of the traffic pattern on the channel. Active jammers are usually effective because they keep the channel busy all the time. These methods are relatively easy to detect. An alternative approach to jamming wireless communication is to employ a reactive strategy. For the reactive jammer, it takes the view point that it is not necessary to jam the channel when nobody is communicating. Instead, the jammer stays quiet when the channel is idle, but starts transmitting a radio signal as soon as it senses activity on the channel. As a result, a reactive jammer targets the reception of a message. It would like to point out that a reactive jammer does not necessarily conserve energy because the jammer's radio must continuously be on in order to sense the channel. The primary advantage for a reactive jammer, however, is that it may be harder to detect.

III. PROBLRM STATEMENT

Consider the scenario depicted in Nodes A and B communicate via a wireless link. Within the communication range of both A and B, there is a jamming node J. When A transmits a packet m to B, node J classifies m by receiving only the first few bytes of m. J then corrupts m beyond recovery by interfering with its reception at B. We address the problem of preventing the jamming node from classifying m in real time, thus mitigating J's ability to perform selective jamming. Our goal is to transform a selective jammer to a random one. Note that in the present work, we do not address packet classification methods based on protocol semantics, as describe.

IV. PROPOSED WORK

Here the contribution towards jamming attacks is reduced by using the two algorithms 1) Symmetric encryption algorithm 2) Brute force attacks against block encryption algorithms The proposed algorithm keeps these two in mind as they are essential in reducing the jamming attacks by using the packet hiding mechanism. In this paper, we address the problem of jamming under an internal threat model. We consider a sophisticated adversary who is aware of network secrets and the implementation details of network protocols at any layer in the network stack. The adversary exploits his internal knowledge for launching selective jamming attacks in which specific messages of "high importance" are targeted. For example, a jammer can target route-request/route-reply messages at the routing layer to prevent route discovery, or target TCP acknowledgments in a TCP session to severely degrade the throughput of an end-to-end flow to launch selective jamming attacks, the adversary must be capable of implementing a classify-then-jam strategy before the completion of a wireless transmission. Such strategy can be actualized either by classifying transmitted packets using protocol semantics, or by decoding Packets on the fly. In the latter method, the jammer may decode

the first few bits of a packet for recovering useful packet identifiers such as packet type, source and destination address. After classification, the adversary must induce a sufficient number of bit errors so that the packet cannot be recovered at the receiver. Selective jamming requires an intimate knowledge of the physical layer, as well as of the specifics of upper layers

A. Network model

The network consists of a collection of nodes connected via wireless links. Nodes may communicate directly if they are within communication range, or indirectly via multiple hops. Nodes communicate both in unicast mode and broadcast mode. Communications can be either unencrypted or encrypted. For encrypted broadcast communications, symmetric keys are shared among all intended receivers. These keys are established using presaged pair wise keys or asymmetric cryptography.

B. Real Time Packet Classification

Consider the generic communication system depicted in Fig. At the PHY layer, a packet m is encoded, interleaved, and modulated before it is transmitted over the wireless channel. At the receiver, the signal is demodulated, DE interleaved, and decoded, to recover the original packet m. Moreover, even if the encryption key of a hiding scheme were to remain secret, the static portions of a transmitted packet could potentially lead to packet classification. This is because for computationally-efficient encryption methods such as block encryption, the encryption of a prefix plaintext with the same key yields a static cipher text prefix. Hence, an adversary who is aware of the underlying protocol specifics (structure of the frame) can use the static cipher text portions of a transmitted packet to classify it.

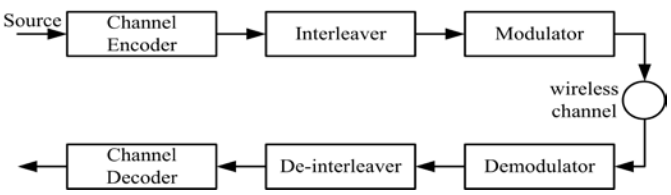

Fig 3:classification of real time packet

We propose a strong hiding commitment scheme (SHCS), which is based on symmetric cryptography. Our main motivation is to satisfy the strong hiding property while keeping the computation and communication overhead to a minimum.

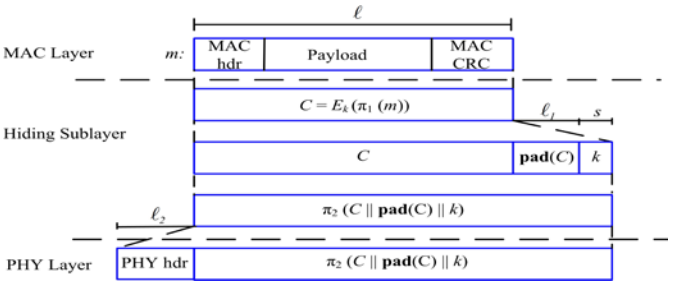

Fig4: processing at hiding sub layer

The computation overhead of SHCS is one symmetric encryption at the sender and one symmetric decryption at the receiver. Because the header information is permuted as a trailer and encrypted, all receivers in the vicinity of a sender must receive the entire packet and decrypt it, before the packet type and destination can be determined. However, in wireless protocols such as 802.11, the complete packet is received at the MAC layer before it is decided if the packet must be discarded or be further processed. If some parts of the MAC header are deemed not to be useful information to the jammer, they can remain unencrypted in the header of the packet, thus avoiding the decryption operation at the receiver

Cryptographic Puzzle Hiding Scheme

We present a packet hiding scheme based on cryptographic puzzles. The main idea behind such puzzles is to force the recipient of a puzzle execute a pre-defined set of computations before he is able to extract a secret of interest. The time required for obtaining the solution of a puzzle depends on its hardness and the computational ability of the solver. The advantage of the puzzle based scheme is that its security does not rely on the PHY layer parameters. However, it has higher computation and communication overhead We consider several puzzle schemes as the basis for CPHS.

Hiding based on All-Or-Nothing Transformation

The packets are pre-processed by an AONT before transmission but remain unencrypted. The jammer cannot perform packet classification until all pseudo-messages corresponding to the original packet have been received and the inverse transformation has been applied. Packet m is partitioned to a set of x input blocks m = {m1, m2, m3….}, which serve as an input to an The set of pseudo-messages m = {m1, m2, m3,…..} is transmitted over the wireless medium Recently Rivets motivated by different security concerns arising in the context of block ciphers, introduced an intriguing primitive called the *All-Or-Nothing Transform (***AONT***)*. An AONT is an efficiently computable transformation Ton strings such that
For any string x, given *all* of T(x), one can efficiently recover x There exists some threshold such that any polynomial time adversely that learns all but bits of T(x) obtains no information about X.
The AONT solves the problem of partial key exposure: Rather than storing a secret key directly, we store the AONT applied to the secret key. If we can build an AONT where the threshold value `is very small compared to the size of the output of the AONT, we obtain security against almost total exposure. Notice that this methodology applies to secret keys with arbitrary structure, and thus protects all kinds of cryptographic systems. One can also consider AONT's that have a two-part output: a public output that doesn't need to be protected, and a secret output that has the exposure-resilience property stated above. Such a notion would also provide the kind of protection we seek to achieve. The AONT has many other applications, as well, such as enhancing the security of block-ciphers and making fixed-block size encryption schemes more efficient [16]. For an excellent exposition on these and other applications of the AONT

V. CONCLUSION

An internal adversary model in which the jammer is part of the network under attack, thus being aware of the protocol specifications and shared network secrets and we showed that the jammer can classify transmitted packets in real time by decoding the first few symbols of an ongoing transmission. We evaluated the impact of selective jamming attacks on network protocols such as TCP and routing. Our findings show that a selective jammer can significantly impact performance with very low effort. We developed three schemes that transform a selective jammer to a random one by preventing real-time packet classification.

VI. REFERENCES

[1] B. Thapa, G. Noubir, R. Rajaramanand, and B. Sheng, "On the Robustness of IEEE802.11 Rate Adaptation Algorithms against Smart Jamming," Proc. ACM Conf. Wireless Network Security (WiSec), 2011.

[2] Y.W. Law, M. Palaniswami, L.V. Hoesel, J. Doumen, P. Hartel, anD P. Havinga, "Energy-Efficient Link-Layer Jamming Attacks against WSN MAC Protocols," ACM Trans. Sensor Networks, vol. 5, no. 1, pp. 1-38, 2009.

[3] L. Lazos, S. Liu, and M. Krunz, "Mitigating Control-Channel Jamming Attacks in Multi-Channel Ad Hoc Networks," Proc. Second ACM Conf. Wireless Network Security, pp. 169-180,
2009.

[4] Y. Liu, P. Ning, H. Dai, and A. Liu, "Randomized Differential DSSS: Jamming-Resistant Wireless Broadcast Communication," Proc. IEEE INFOCOM, 2010.

[5] B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons, 2007.

Mrs. Madhavi Latha. Y (M.Tech-CSE), Nimra Institute of Engineering & Technology, Ongole.

Mr. Rambabu Pemula Received B.Tech(CSE), M.Tech(SE) from JNTU Hyderabad and MBA from ANU Guntur. Presently working as Associate Professor at Nimra Institute of Engineering & Technology, Ongole.